Name Laurence D. King
Address 1999 Harrison Street, Suite 1560
City, State, Zip Oakland, CA 94612
Phone 415-772-4700
Fax 415-772-4707
E-Mail lking@kaplanfox.com

☐ FPD ☐ Appointed ☐ CJA ☐ Pro Per ☒ Retained

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

In re: Illuminate Education Data Security Incident Litigation PLAINTIFF(S), v. DEFENDANT(S).	CASE NUMBER: 8:22-cv-01164-JVS-ADSx **NOTICE OF APPEAL**

NOTICE IS HEREBY GIVEN that Anastasiya Kisil, Lucas Cranor, Sarah Chung, Kristen Weiland, Lorraine Deniz, Tara Chambers, and Janene Vitro hereby appeals to the United States Court of Appeals for the Ninth Circuit from:

Name of Appellant

Criminal Matter

☐ Conviction only [F.R.Cr.P. 32(j)(1)(A)]
☐ Conviction and Sentence
☐ Sentence Only (18 U.S.C. 3742)
☐ Pursuant to F.R.Cr.P. 32(j)(2)
☐ Interlocutory Appeals
☐ Sentence imposed:

☐ Bail status:

Civil Matter

☒ Order (specify): 114

☐ Judgment (specify):

☐ Other (specify):

Imposed or Filed on _____. Entered on the docket in this action on 11/8/2023.

A copy of said judgment or order is attached hereto.

December 4, 2023
Date

/s/ *Laurence D. King*
Signature

☐ Appellant/ProSe ☒ Counsel for Appellant ☐ Deputy Clerk

Note: The Notice of Appeal shall contain the names of all parties to the judgment or order and the names and addresses of the attorneys for each party. Also, if not electronically filed in a criminal case, the Clerk shall be furnished a sufficient number of copies of the Notice of Appeal to permit prompt compliance with the service requirements of FRAP 3(d).

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 6. Representation Statement

Instructions for this form: http://www.ca9.uscourts.gov/forms/form06instructions.pdf

Appellant(s) *(List **each** party filing the appeal, do not use "et al." or other abbreviations.)*

Name(s) of party/parties:

Anastasiya Kisil, Lucas Cranor, Sarah Chung, Kristen Weiland, Lorraine Deniz, Tara Chambers, Janene Vitro

Name(s) of counsel (if any):

Kaplan Fox & Kilsheimer LLP
Laurence D. King, Matthew B. George, Blair E. Reed

Address: 1999 Harrison Street, Suite 1560, Oakland, CA 94612

Telephone number(s): 415-772-4700

Email(s): lking@kaplanfox.com; mgeorge@kaplanfox.com; breed@kaplanfox.com

Is counsel registered for Electronic Filing in the 9th Circuit? ◉ Yes ○ No

---

Appellee(s) *(List only the names of parties and counsel who will oppose you on appeal. List separately represented parties separately.)*

Name(s) of party/parties:

Illuminate Education, Inc. d/b/a Pupil Path

Name(s) of counsel (if any):

Kirkland & Ellis LLP
Tammy Tsoumas

Address: 2049 Century Park East, Suite 3700, Los Angeles, CA 90067

Telephone number(s): (310) 552-4200

Email(s): tammy.tsoumas@kirkland.com

To list additional parties and/or counsel, use next page.

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

Continued list of parties and counsel: *(attach additional pages as necessary)*

Appellants

Name(s) of party/parties:

Name(s) of counsel (if any):

Kantrowitz, Goldhamer & Graifman P. C.
Melissa R. Emert, Gary S. Graifman

Address: 135 Chestnut Ridge Road, Suite 200 Montvale, NJ 07645

Telephone number(s): 201-391-7000

Email(s): memert@kgglaw.com; ggraifman@kgglaw.com

Is counsel registered for Electronic Filing in the 9th Circuit? ○ Yes ◉ No

Appellees

Name(s) of party/parties:

Name(s) of counsel (if any):

Kirkland & Ellis LLP
Devin S. Anderson, Emily M. Long

Address: 1301 Pennsylvania Avenue, NW, Washington DC 20004

Telephone number(s): 202-389-5000

Email(s): devin.anderson@kirkland.com; emily.long@kirkland.com

Name(s) of party/parties:

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	8:22-cv-01164-JVS (ADSx)	Date	November 6, 2023
Title	In re: Illuminate Education Data Security Incident Litigation		

Present: The Honorable	**James V. Selna, U.S. District Court Judge**

Elsa Vargas	Not Present
Deputy Clerk	Court Reporter
Attorneys Present for Plaintiffs:	Attorneys Present for Defendants:
Not Present	Not Present

Proceedings: **[IN CHAMBERS] Order Regarding Motion to Dismiss [93] [PUBLIC VERSION]**

Defendant Illuminate Education, Inc. ("Illuminate") moved to dismiss the Consolidated Amended Complaint ("CAC"). (Mot., Dkt. No. 97 (sealed).) Plaintiffs[1] opposed the motion. (Opp'n, Dkt. No. 102 (sealed).) Illuminate replied. (Reply, Dkt. No. 112 (sealed).) In advance of the hearing, the Court distributed a tentative ruling to the parties on November 3, 2023, and the parties submitted on the tentative. (Dkt. No. 113.) Accordingly, the Court vacated oral argument. Fed. R. Civ. P. 78; L.R. 7-15.

For the foregoing reasons, the Court **GRANTS in part** and **DENIES in part as moot** the motion to dismiss without leave to amend.

I. BACKGROUND

Illuminate is a software company that services 17 million students in 5,200 schools and districts across all 50 states. (CAC, Dkt. No. 85 ¶¶ 2–3.) Illuminate offers several products that require the collection of students' personal information, including names, birth dates, class schedules, behavioral records, and health and socioeconomic information. (Id. ¶¶ 4–6.) On January 8, 2022, Illuminate became aware that an unauthorized third party gained access to Illuminate's databases containing personally identifiable information ("PII") and protected health information ("PHI") of students.

[1] Plaintiffs are Lucas Cranor ("Cranor"), Kristen Weiland ("Weiland"), Anastasiya Kisil ("Kisil"), Tara Chambers ("Chambers"), Janene Vitro ("Vitro"), and Lorraine Deniz ("Deniz") (collectively, "Plaintiffs"). Plaintiffs bring this action individually and on behalf of all others similarly situation. (See Consolidated Amended Complaint ("CAC"), Dkt. No. 85 (sealed).)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. 8:22-cv-01164-JVS (ADSx) Date November 6, 2023

Title In re: Illuminate Education Data Security Incident Litigation

(Id. ¶ 8.) [redacted] (Id.) Illuminate conducted an investigation and confirmed unauthorized access took place between December 28, 2021, and January 8, 2022 (the "Data Breach"). (Id. ¶ 10.) The Data Breach was a result of an unauthorized access to one of Illuminate's platforms used in K-12 school districts. (Id. ¶ 27.) Information leaked included student academic, behavior, and demographic information. (Id. ¶ 44 (listing the information leaked).) The Data Breach affected over three million students, primarily students enrolled during 2021–2022, and possibly as early as 2016. (Id. ¶¶ 42–43.) Illuminate did not notify schools until late March 2022. (Id. ¶ 28.) Plaintiffs bring this action individually and on behalf of other class members. (Id. ¶ 12.)

II. LEGAL STANDARD

A. Motion to Dismiss Pursuant to Rule 12(b)(1)

Dismissal is proper when a plaintiff fails to properly plead subject matter jurisdiction in the complaint. Fed. R. Civ. P. 12(b)(1). A "jurisdictional attack may be facial or factual." Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). If the challenge is based solely upon the allegations in the complaint (a "facial attack"), the court generally presumes the allegations in the complaint are true. Id.; Warren v. Fox Family Worldwide, Inc., 328 F.3d 1136, 1139 (9th Cir. 2003). If instead the challenge disputes the truth of the allegations that would otherwise invoke federal jurisdiction, the challenger has raised a "factual attack," and the court may review evidence beyond the confines of the complaint without assuming the truth of the plaintiff's allegations. Safe Air, 373 F.3d at 1039. The plaintiff bears the burden of establishing subject matter jurisdiction. Kokkonen v. Guardian Life Ins. Co. of Am., 511 U.S. 375, 377 (1994).

Pursuant to Article III of the Constitution, the Court's jurisdiction over the case "depends on the existence of a 'case or controversy.'" GTE Cal., Inc. v. FCC, 39 F.3d 940, 945 (9th Cir. 1994). A "case or controversy" exists only if a plaintiff has standing to bring the claim. Nelson v. NASA, 530 F.3d 865, 873 (9th Cir. 2008), rev'd on other grounds, 562 U.S. 134 (2011). To have standing, "a plaintiff must show (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative,

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	8:22-cv-01164-JVS (ADSx)	Date	November 6, 2023
Title	In re: Illuminate Education Data Security Incident Litigation		

that their injury will be redressed by a favorable decision." Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc., 528 U.S. 167, 180–81 (2000); see also Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992); Nelson, 530 F.3d at 873. "[P]laintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2208 (2021).

B. Motion to Dismiss Pursuant to Rule 12(b)(6)

Under Rule 12(b)(6), a defendant may move to dismiss for failure to state a claim upon which relief can be granted. A plaintiff must state "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim has "facial plausibility" if the plaintiff pleads facts that "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

In resolving a 12(b)(6) motion under Twombly, the Court must follow a two-pronged approach. First, the Court must accept all well-pleaded factual allegations as true, but "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Iqbal, 556 U.S. at 678. Nor must the Court "'accept as true a legal conclusion couched as a factual allegation.'" Id. at 678–80 (quoting Twombly, 550 U.S. at 555). Second, assuming the veracity of well-pleaded factual allegations, the Court must "determine whether they plausibly give rise to an entitlement to relief." Id. at 679. This determination is context-specific, requiring the Court to draw on its experience and common sense, but there is no plausibility "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct." Id.

III. DISCUSSION

A. Motion to Dismiss Pursuant to Rule 12(b)(1)

An injury, for the purposes of standing, is concrete when it is "real, and not abstract." TransUnion LLC, 141 S. Ct. at 2204. Illuminate argues Plaintiffs' four theories of harm are still insufficient to establish a concrete injury. (Mot. at 4–13.)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. 8:22-cv-01164-JVS (ADSx) Date November 6, 2023

Title In re: Illuminate Education Data Security Incident Litigation

1. Whether Plaintiffs Plausibly Alleged Actual Identity Theft

Illuminate argues that "[j]ust like last time, plaintiffs make no allegations suggesting that their minor student children suffered any actual identity theft, meaning that identity theft is not an available theory of harm for those individuals." (Mot. at 6.) The Court agrees. As this Court found in its prior Order, "Plaintiffs do not allege social security, credit card, or bank information was leaked." (Order, Dkt. No. 79, at 4.) Plaintiffs still fail to allege such information was leaked. (See generally CAC.) The CAC even notes that "Illuminate state[d] in the Data Breach notices that Social Security numbers were not impacted by the Data Breach." (Id. ¶¶ 178, 187, 199, 211, 222, 233.) Moreover, Vitro's allegation that someone charged her debit card on a fake website is still insufficient to establish standing because the CAC still fails to explain how any information that was leaked could be linked to the debit card charge. Lastly, Plaintiffs merely reallege receiving unwanted spam emails and text messages. (Id. ¶¶ 177, 186, 207, 218, 234.) Thus, as in its prior Order, this Court is left to speculate, based on the allegations and facts, as to whether any actual identity theft occurred based on information leaked in the Data Breach.

Plaintiffs rely on TransUnion LLC, 141 S. Ct. 2190, for support. Specifically, Plaintiffs argue that "[v]arious intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." TransUnion LLC, 141 S. Ct. 2204. However, a "concrete" injury "may include tangible or intangible harms, so long as they actually exist and are real, and not abstract." I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1046 (N.D. Cal. 2022). Thus, "[a] real, existing injury is a prerequisite to federal jurisdiction because 'federal courts do not adjudicate hypothetical or abstract disputes,' nor do they 'exercise general legal oversight . . . of private entities.'" Id. at 1046 (quoting TransUnion LLC, 141 S. Ct. 2203). It is unclear whether any "real" harm exists because [redacted] (CAC ¶ 29.) [redacted] (Id.) [redacted] (See id. ¶¶ 176, 185, 197, 209, 220

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	8:22-cv-01164-JVS (ADSx)	Date	November 6, 2023
Title	In re: Illuminate Education Data Security Incident Litigation		

(alleging that "children's Private Information may be available for sale on the dark web").) Thus, Plaintiffs still fail to allege any real, existing harm from the alleged disclosure of private information, which only included the students' academic, behavior, and demographic information.

Moreover, Plaintiffs cite various factually distinguishable cases that are inapplicable to the present case. See, e.g., Wynn v. Audi of Am., No. 21-cv-8518, 2022 WL 2916341, at *1 (N.D. Cal. July 25, 2022) (finding that plaintiff alleged "names, home and business addresses, email addresses, driver's license numbers, social security numbers, dates of birth, account and loan numbers, and tax identification numbers" were leaked); Bohnak v. Marsh & McLennan Companies, Inc., 79 F.4th 276, 280 (2d Cir. 2023) (alleging that "Social Security or other federal tax identification number[s], driver's license or other government issued identification, and passport information" was leaked); Medoff v. Minka Lighting, LLC, No. 2:22-cv-8885, 2023 WL 4291973, at *1 (C.D. Cal. May 8, 2023) (alleging that the social security numbers of employees was posted on the internet); Leonard v. McMenamins, Inc., No. 2:22-cv-94, 2022 WL 4017674, at *1 (W.D. Wash. Sept. 2, 2022) (alleging that the leaked information included "name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts"); In re USAA Data Sec. Litig., 621 F. Supp. 3d 454, 462 (S.D.N.Y. 2022) (alleging misuse of driver's license numbers to open financial accounts); Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, Dkt. No. 11, at 7 (D. Ariz. 2021) (alleging that the personal information included names, addresses, employee ID numbers, and W-2 or 1099 details, such as Social Security numbers).

Accordingly, Plaintiffs still fail to establish standing based on actual identity theft.

2. Whether Plaintiffs Plausibly Alleged a Material Risk of Future Identity Theft

With respect to damages, in its prior Order, the Court held that "Plaintiffs' allegations do not demonstrate that the risk of future harm materialized." (Order at 6 (internal quotation marks omitted)). Moreover, the Ninth Circuit recently recognized that "the Supreme Court is clear that where a risk of future harm has not yet materialized, the 'plaintiffs' argument for standing for their damages claims based on an asserted risk of

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	8:22-cv-01164-JVS (ADSx)	Date	November 6, 2023
Title	In re: Illuminate Education Data Security Incident Litigation		

future harm is unavailing.'" Bock v. Washington, 33 F.4th 1139, 1145 (9th Cir. 2022) (quoting TransUnion LLC, 141 S. Ct. at 2211). As mentioned above, Plaintiffs still fail to establish any actual identity theft related to the Data Breach. Thus, the risk of future harm has not materialized. Plaintiffs fail to address this argument in their Opposition. (See generally Opp'n.)

With respect to injunctive relief, the Court found that "Plaintiffs do not explain how the information leaked in the Data Breach creates a risk that is imminent and substantial." (Order at 7.) Plaintiffs' CAC still does not explain how students' academic, behavioral, and demographic information creates an imminent and substantial risk. (See generally CAC.) As Illuminate notes, "[t]he types of data at issue did not change between the original and amended complaints." (Reply at 3.) Rather, Plaintiffs continue to allege conclusorily that a substantial risk of identify theft and fraud exists based on news articles. (Id. ¶¶ 118–31.) For instance, Plaintiffs cite a Joint Cybersecurity Advisory issued by the FBI that states "K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers." (Id. ¶ 128.) But such conclusory statements do not explain how the information leaked creates a substantial risk to these Plaintiffs who have not suffered any actual harm.

Plaintiff argue that "post-TransUnion cases have found Article III Standing where plaintiffs have alleged that their private information has been disclosed to cybercriminals."[2] (Opp'n at 10.) However, in its Opposition, Plaintiff relies on the same cases that this Court previously found unhelpful. (See Order at 6–7.) And the new cases Plaintiffs cite do not support their position. In In re Pawn America Consumer Data Breach Litig., No. 21-cv-2554, 2022 WL 3159874, at *1–3 (D. Minn. Aug. 8, 2022), plaintiffs alleged that the stolen information included "customers' full names, birth dates, Social Security numbers, driver's-license numbers, passport numbers, other government-issued identification numbers, and financial-account information," and the court found that plaintiffs failed to allege a "sufficiently imminent and substantial" risk of future harm. The court noted that "every human being has an interest in ensuring that any entity that possesses his or her private information keeps that information safe. The

[2] In their Opposition, Plaintiffs also cited other cases in support of their position, but the Court finds those cases unpersuasive because they were decided before TransUnion LLC. (See Opp'n at 10–15.)

universal interest in the security of one's private data does not equate to a substantial and imminent risk of harm." Id. at *3. In Bohnak, plaintiffs alleged that "Social Security or other federal tax identification number[s], driver's license or other government issued identification, and passport information" was leaked. 79 F.4th at 280. The court also acknowledged that "while not a necessary component of establishing standing, courts have been more likely to conclude that a plaintiff has established a substantial risk of future injury where some part of the compromised dataset has been misused—even if a plaintiff's own data has not." Id. at 288 (internal quotation marks and citations omitted). However, in this case, Plaintiffs do not allege any misuse of the students' leaked information. (See generally CAC). Moreover, Plaintiffs admit that their "data has not been misused" in their Opposition. (Opp'n at 11.) Moreover, in Bohnak, the court "explained that courts may consider whether the exposed PII is of the type more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed. On one hand, we noted that the dissemination of high-risk information such as [Social Security Numbers] . . . especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud. On the other hand, we reasoned that the exposure of data that is publicly available, or that can be rendered useless (like a credit card number unaccompanied by other PII), is less likely to subject plaintiffs to a perpetual risk of identity theft." 79 F.4th at 288. As previously mentioned, plaintiffs do not allege that their social security numbers, credit card information, or other bank account information was leaked. In Salas v. Acuity-CHS, LLC, No. 22-317, 2023 WL 2710180, at *1 (D. Del. Mar. 30, 2023), plaintiffs alleged that their names, dates of birth, and Social Security numbers were compromised. In Salas, the court found that plaintiff "alleged a future injury that is sufficiently imminent" since she "allege[d] actual misuse of her private information" that was "for sale to criminals on the dark web." 2023 WL 2710180, at *4 (internal quotation marks and citations omitted). Specifically, the plaintiff in Salas alleged that "she received an alert through her identity theft monitoring service that her email address had recently been used in a potential identity theft incident." Id. Lastly, the court in Salas also noted that "the nature of the information [t]here is sensitive," as "social security numbers, birth dates, and names" are "more likely to create a risk of identity theft or fraud if compromised." Id. at *4 (internal quotation marks and citations omitted).

[redacted]

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. 8:22-cv-01164-JVS (ADSx) Date November 6, 2023

Title In re: Illuminate Education Data Security Incident Litigation

[redacted][3]

Accordingly, Plaintiff still fail to establish standing where the harm is based on risk of future identity theft and fraud.

3. Whether Plaintiffs Plausibly Alleged Harms Derived of the Allegations of Future Harm

In its prior Order, this Court held that "[t]o the extent Plaintiffs allegations relate to mitigation measures for possible future harms or identity theft, such allegations fail to establish standing." (Order at 8.) In their Opposition, Plaintiffs argue that "[f]ollowing TransUnion [LLC], courts across the country have recognized that harms that result as a consequence of a plaintiff's knowledge of a substantial risk of identity theft, including time and money spent responding to a data breach or emotion[al] distress can satisfy concreteness." (Opp'n at 14 (quoting Medoff, 2023 WL 4291973, at *4)). But as Medoff further explains, "[t]hese additional harms, however, can only qualify as concrete injuries in fact when they are based on a risk of harm that is either certainly impending or substantial." 2023 WL 4291973, at *5 (internal quotation marks omitted). "In the absence of an impending or substantial harm, additional harms incurred become the type of self-inflicted injuries that cannot confer standing." Id. For reasons discussed above, Plaintiffs fail to establish any "impending" or "substantial" risk of harm. Accordingly, Plaintiffs additional harms do not qualify as concrete injuries for standing purposes.

[3] Instead, Plaintiffs cite Bohnak for the proposition that "courts have been more likely to conclude that a plaintiff has established a substantial risk of future injury where some part of the compromised dataset has been misused—even if a plaintiff's own data has not." (Opp'n at 13 (quoting Bohnak, 79 F.4th at 288).) However, as previously mentioned, Plaintiffs do not allege that their information has been misused.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. 8:22-cv-01164-JVS (ADSx) Date November 6, 2023

Title In re: Illuminate Education Data Security Incident Litigation

Plaintiffs also argue that Illuminate's delay in notifying them of the Data Breach caused them harm. (Opp'n at 15.) In its prior Order, this Court found that "Plaintiffs' reliance on Stallone v. Farmers Group, No. 2:21-cv-1659, 2022 WL 10091489 (D. Nev. Oct. 15, 2022), [wa]s unpersuasive given the court[']s limited discussion of TransUnion LLC." (Order at 7.) But Plaintiffs continue to rely on Stallone, as it is the only case that Plaintiffs cite to support their assertion. However, Plaintiffs argument still fails because Stallone is inapposite to this case. In Stallone, the court found that plaintiffs adequately alleged an incremental harm caused by delay because "Plaintiff ha[d] alleged an imminent threat of harm." 2022 WL 10091489, at *8 n.4. The Stallone court also found that plaintiffs' "information was stolen, ha[d] already surfaced on the Internet, and been misused by others." Id. at *6. As discussed above, Plaintiffs in this case have not alleged an imminent or substantial risk of harm. Nor have Plaintiffs alleged that the students' information was found online or misused. Thus, Plaintiffs fail to establish how delay in notification of a Data Breach can result in an injury-in-fact.

Accordingly, Plaintiffs have no standing where the harm is based on time lost on mitigation measures or emotional distress or delay in notification.

4. Whether Plaintiffs Plausibly Alleged a Loss of Value of Information or Privacy

With respect to diminution of value, this Court previously held that Plaintiffs failed to sufficiently allege either the existence of a market for personal information or an impairment of an ability to participate in the market for their personal information. (Order at 8–9.) Plaintiffs still fail to do so. Plaintiffs allegations concerning diminution of the value of their private information are entirely conclusory. (CAC ¶¶ 174, 183, 195, 206, 217, 229.) The only new allegation is the single search from April 15, 2022 for purchase of the Illuminate database that was stolen. (Id. ¶ 62.) Plaintiffs argue that "[t]he newly-added allegation of a request on the darknet to purchase the information stolen from Illuminate plainly evidences the existence of a market, [redacted] (Opp'n at 9.) Illuminate argues that "[t]he existence of some hypothetical demand for information does not establish a market in which plaintiffs could derive some pecuniary value through selling their data." (Reply at 7.) The Court agrees. As explained above, Plaintiffs fail to show how one anonymous demand from 18 months ago establishes a market for the information leaked in the Data Breach. Plaintiffs also do

not allege that the information from the Data Breach is available on the dark web. (See generally CAC.)

Plaintiffs continue to only rely on Stallone to support their argument. However, in Stallone, it was "undisputed that Plaintiff sufficiently alleged a market for his PII exists on the dark web." 2022 WL 10091489, at *19 (internal quotation marks omitted). Moreover, the district court in Stallone relied on Pruchnicki v. Envision Healthcare Corp., for the proposition that "[d]iminution in value of personal information can be a viable theory of damages." 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), aff'd 845 Fed. App'x 613 (9th Cir. 2021). However, in Pruchnicki, the district court stated that "[i]n order to survive a motion to dismiss on this theory of damages, a plaintiff 'must establish both the existence of a market for her personal information and an impairment of her ability to participate in that market.'" Id. The district court found that "there are no specific allegations that plaintiff has been unable to sell, profit from, or otherwise monetize her personal information. Similarly, there are no specific allegations suggesting how the value of her personal information has been reduced." Id. at 1235. On appeal, the Ninth Circuit found that plaintiffs did not adequately allege diminution of the value of her personal information. Pruchnicki, 845 Fed. App'x at 614. Specifically, the Ninth Circuit stated that "[a]lthough the studies cited by [plaintiff] establish that personal information may have value in general, [plaintiff] failed to adequately allege that *her* personal information actually lost value. Several courts in this Circuit have found, and we agree, that the 'mere misappropriation of personal information' does not establish compensable damages." Id. at 614–15 (emphasis in original). Thus, the Court declines to follow Stallone because the district court in that case misconstrues the law in the Ninth Circuit. In fact, Stallone cited cases that all predate the district court and appellate court decisions in Pruchnicki to support its assertion that "both the existence of a market for their PII and an impairment of their ability to participate in that market is not supported by Ninth Circuit precedent, and other district courts in this Circuit have rejected them." 2022 WL 10091489, at *18. Moreover, two other district courts in the Ninth Circuit reached the opposite conclusion of Stallone. See, e.g., Wesch v. Yodlee, Inc., No. 20-cv-5991, 2021 WL 6206644, at *5 (N.D. Cal. July 19, 2021) (holding that "[t]o plead facts sufficient to show such a theory of damages[,] a plaintiff must establish both the existence of a market for her personal information and an impairment of her ability to participate in that market" (internal quotation marks omitted)); Durgan v. U-Haul Int'l Inc., No. CV-22-1565, 2023 WL 7114622, at *3 (D. Ariz. Oct. 27, 2023) (stating that "[t]o successfully show harm arising from diminution in PII's value, a plaintiff must establish both the

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. 8:22-cv-01164-JVS (ADSx) Date November 6, 2023

Title In re: Illuminate Education Data Security Incident Litigation

existence of a market for her personal information and an impairment of her ability to participate in that market" (internal quotation marks omitted)). Illuminate argues that "even if plaintiffs' allegations could establish the existence of a market, plaintiffs have again failed to explain how the value of the data at issue—academic, behavioral, and basic demographic information—was somehow diminished to plaintiffs." (Reply at 7.) Plaintiffs do not allege that they lost the ability to use or sell their data because of the Data Breach. (See generally CAC.) Thus, Plaintiffs fail to assert that they have been harmed through the loss of value of their information.

With respect to loss of privacy, this Court previously noted that "other federal courts have similarly rejected the argument that a loss of privacy arising from the theft of non-sensitive personal information, standing alone, supports Article III standing." (Order at 9 (quoting Kim v. McDonald's USA, LLC, No. 21-cv-5287, 2022 WL 4482826, at *5 (N.D. Ill. Sept. 27, 2022).) Illuminate argues that "[t]he amended complaint simply realleges precisely the same categories of information—academic, behavioral, and demographic information—that the Court previously found did 'not sufficiently establish standing.'" (Reply at 8.) The Court agrees. As discussed above, Plaintiffs rely on factually distinguishable cases that involve sensitive personal information or allegations of actual misuse.

Accordingly, Plaintiffs have no standing related to loss of value of information or privacy.

Based on the foregoing, Plaintiffs failed to establish standing. Accordingly, the Court **GRANTS** the motion to dismiss pursuant to Rule 12(b)(1). Because the Court grants the motion to dismiss as to standing, the Court need not analyze Illuminate's motion to dismiss based on failure to state a claim or the choice-of-law analysis. Thus, the Court **DENIES** the motion to dismiss pursuant to Rule 12(b)(6) as moot.

B. Leave to Amend

Given the 18 months since the notification of the Data Breach, the discovery available before repleading their allegations, [redacted], the Court finds that Plaintiffs will not be able to correct the deficiencies in their CAC. Nor have Plaintiffs cured the deficiencies identified in the Court's prior Order. Thus, the Court finds that granting

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. 8:22-cv-01164-JVS (ADSx) Date November 6, 2023

Title In re: Illuminate Education Data Security Incident Litigation

leave to amend would be futile. See Cervantes v. Countrywide Home Loans, Inc., 656 F.3d 1034, 1041 (9th Cir. 2011) (setting forth the standard of review and stating that leave to amend may be denied where amendment would be futile); Armstrong v. Reynolds, 22 F.4th 1058, 1071 (9th Cir. 2022) ("[P]laintiffs should be granted leave to amend their complaints unless it is clear, upon de novo review, that the complaint could not be saved by any amendment." (internal citations omitted)).

Accordingly, the Court **DENIES** Plaintiffs leave to amend.

IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS in part** and **DENIES in part as moot** the motion to dismiss without leave to amend.

IT IS SO ORDERED.